[1]

EQUATIONS OF SHIMURA CURVES OF GENUS 2

JOSEP GONZÁLEZ, VICTOR ROTGER

Abstract. We present explicit models for Shimura curves X_D and Atkin-Lehner quotients $X_D/\langle\omega_m\rangle$ of them of genus 2. We show that several equations conjectured by Kurihara are correct and compute for them the kernel of Ribet's isogeny $J_0(D)^{new} \to J_D$ between the new part of the Jacobian of the modular curve $X_0(D)$ and the Jacobian of X_D.

1. Introduction

Let B_D be the indefinite quaternion algebra over $\mathbb{Q}$ of reduced discriminant $D = p_1 \cdot ... \cdot p_{2r}$ for pairwise different prime numbers p_i and let $X_D/\mathbb{Q}$ be the Shimura curve attached to B_D. As it was shown by Shimura [23], X_D is the coarse moduli space of abelian surfaces with quaternionic multiplication by B_D.

Let $W = \{\omega_m : m \mid D\} \subseteq \mathrm{Aut}_{\mathbb{Q}}(X_D)$ be the group of Atkin-Lehner involutions. For any $m \mid D$, we shall denote $X_D^{(m)} = X_D/\langle\omega_m\rangle$ the quotient of the Shimura curve X_D by ω_m. The importance of the curves $X_D^{(m)}$ is enhanced by their moduli interpretation as curves embedded in Hilbert-Blumenthal surfaces and Igusa's threefold $\mathcal{A}_2$ (cf. [21], [22]).

The classical modular case arises when $D = 1$. In this case, automorphic forms of these curves admit Fourier expansions around the cusp of infinity and we know explicit generators of the field of functions of such curves. Also, explicit methods are known to determine bases of the space of regular differentials of them, which are used to compute equations for quotients of modular curves.

When $D \neq 1$, the absence of cusps has been an obstacle for explicit approaches to Shimura curves. Explicit methods to handle with functions and regular differential forms on these curves are less accessible and we refer the reader to [3] for progress in this regard. For this reason, at present few equations of Shimura curves are known, all of them of genus 0 or 1 (cf. [13], [11], [6]). In addition, in a later work, Kurihara conjectured equations for all Shimura curves of genus 2 and for several curves of genus 3 and 5, though he was not able to give a proof for his guesses (cf. [14]).

In this paper, we present equations for thirteen genus two bielliptic Shimura curves and Atkin-Lehner quotients of them.

In particular, we prove that the equations suggested in [14] for X_{26}, X_{38} and X_{58} are unconditionally correct. In turn, this has allowed us to explicitly determine the kernel of Ribet's isogeny $J_0(D)^{new} \to \mathrm{Jac}(X_D)$ and to prove that Ogg's prediction in [17] is also correct for these cases.

[1]The first author is supported in part by DGICYT Grant BFM2000-0794-C02-02 and the second author is partially supported by Ministerio de Ciencia y Tecnología BFM2000-0627

1991 *Mathematics Subject Classification.* 11G18, 14G35.

Key words and phrases. Shimura curve, bielliptic curve.

The remaining 10 curves presented here are the only bielliptic curves $X_D^{(m)}$, $m \neq 1$, of genus 2. Phrased in other terms, this is the complete list of all genus two curves $X_D^{(m)}$ whose hyperelliptic involution is not of Atkin-Lehner type. Note that a phenomenon of this kind was already encountered in the modular setting by the curve $X_0(37)$. Our method can also be used to determine equations for genus two bielliptic Shimura curves with nontrivial Γ_0-level structure, of which there exist 89. For the sake of brevity, these will not be considered in this work.

2. Explicit models of bielliptic curves of genus 2

Proposition 2.1. *Let C be a genus two curve defined over a field k of characteristic not 2 or 3 and w its hyperelliptic involution. Assume $\mathrm{Aut}_k(C)$ contains a subgroup $\langle u_1, u_2 = u_1.w\rangle$ isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$ and let us denote by C_{u_i} the elliptic quotient $C/\langle u_i\rangle$. If the two elliptic curves*

$$E_1 : Y^2 = X^3 + A_1X + B_1\,, \quad E_2 : Y^2 = X^3 + A_2X + B_2\,,$$

are isomorphic to C_{u_1} and C_{u_2} resp. over k, then C admits a hyperelliptic equation of the form $y^2 = ax^6 + bx^4 + cx^2 + d$, where $a \in k^*$, $b \in k$ are solutions of the following system:

$$(1) \qquad \left\{ \begin{array}{rcl} 27a^3B_2 & = & 2A_1^3 + 27B_1^2 + 9A_1B_1b + 2A_1^2b^2 - B_1b^3 \\ 9a^2A_2 & = & -3A_1^2 + 9B_1b + A_1b^2 \end{array} \right. ,$$

$c = (3A_1 + b^2)/(3a)$, $d = (27B_1 + 9A_1b + b^3)/(27a^2)$ and the involution u_1 on C is given by $(x, y) \mapsto (-x, y)$.

Proof. If C has a nonhyperelliptic involution u_1 defined over k, then C/k admits an equation of the form

$$(2) \qquad y^2 = ax^6 + bx^4 + cx^2 + d\,, \quad a, b, c, d \in k\,,$$

and the involution u_1 acts sending $(x, y) \mapsto (-x, y)$. Indeed, due to the fact that the morphisms $C \to C/\langle u_i\rangle$ are defined over k there are $\omega_1, \omega_2 \in H^0(C, \Omega^1_{C/k})$ such that $u_1^*\omega_1 = \omega_1$, $u_1^*\omega_2 = -\omega_2$. The functions $x = \omega_1/\omega_2$, $y = dx/\omega_2$ must satisfy a relation of the form $y^2 = f(x)$, where $f \in k[x]$ has degree 5 or 6 and does not have double roots (see Proposition 2.1 in [7]). Then, $u_1^*(x) = -x$ and $u_1^*(y) = y$. It follows $f(-x) = x$ and, in particular, $\deg f = 6$.

Given an equation for C as (2), the elliptic curves

$$C_1 : Y^2 = aX^3 + bX^2 + cX + d\,, \quad C_2 : Y^2 = dX^3 + cX^2 + bX + a$$

are k-isomorphic to C_{u_1} i C_{u_2} respectively, due to the fact that the nonconstant morphisms $\pi_1 : C \to C_1$, $(x, y) \mapsto (x^2\,, y)$ i $\pi_2 : C \to C_2$, $(x, y) \mapsto (1/x^2\,,\ y/x^3)$ are defined over k and satisfy $\pi_i \circ u_i = \pi_i$, $i \leq 2$. Therefore, every curve C_{u_i} is isomorphic over k to the curve $Y^2 = X^3 + A_{u_i}X + B_{u_i}$, where

$$(3) \qquad \left\{ \begin{array}{ll} A_{u_1} = -b^2/3 + a.c\,, & B_{u_1} = 2\,b^3/27 - a.b.c/3 + a^2.d\,, \\ A_{u_2} = -c^2/3 + b.d\,, & B_{u_2} = 2\,c^3/27 - b.c.d/3 + a.d^2\,, \end{array} \right.$$

and, thus, there exist $\mu_i \in k^*$, $i \leq 2$, such that:

$$A_{u_i}\mu_i^4 = A_i\,, \quad B_{u_i}\mu_i^6 = B_i\,.$$

It can be easily checked that the curve

$$y^2 = a\frac{\mu_1^4}{\mu_2^2}x^6 + b\mu_1^2x^4 + c\mu_2^2x^2 + d\frac{\mu_2^4}{\mu_1^2}$$

is k-isomorphic to C. The statement is an immediate consequence of rewriting the system (3) for this equation, since $a \neq 0$ and now $A_{u_i} = A_i$, $B_{u_i} = B_i$. $\square$

Remark 2.1. *Given two elliptic curves E_1, E_2 over k and a group isomorphism $\psi : E_1[2](\bar{k}) \to E_2[2](\bar{k})$ which is not the restriction of an isomorphism between E_1 and E_2 over $\bar{k}$, Proposition 4 in* [9] *yields a genus two curve $C/\bar{k}$ such that* $\operatorname{Jac} C \simeq (E_1 \times E_2)/\{(P, \psi(P)) : P \in E_1[2]\}$.

In our case, when we consider the elliptic curves defined over k

$$C_1 : Y^2 = aX^3 + bX^2 + cX + d\,, \quad C_2 : Y^2 = dX^3 + cX^2 + bX + a$$

and the isomorphism of G_k-modules $\psi : C_1[2](\bar{k}) \to C_2[2](\bar{k})$, $(x, 0) \mapsto (1/x, 0)$, the formula of the quoted proposition yields a curve which is shown to be isomorphic to $C : y^2 = ax^6 + bx^4 + cx^2 + d$ over k.

Hence, system (1) can be viewed as a different way to collect all curves C obtained from all ψ as above. By Proposition 3 of [9]*, if $E_1 \not\simeq E_2$ over $\bar{k}$, the system has six different solutions $(a, b, c, d) \in \bar{k}^4$ and there is a unique solution defined over k if and only $(E_1 \times E_2)(\bar{k})$ has a unique nontrivial G_k-stable subgroup G isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$, and in this case* $\operatorname{Jac} C = (E_1 \times E_2)/G$*. Here, by the trivial G_k-stable subgroups, we mean $E_1[2](\bar{k}) \times \{0\}$ and $\{0\} \times E_2[2](\bar{k})$.*

3. Shimura curves of genus two

Let B be an indefinite quaternion algebra over $\mathbb{Q}$ of discriminant D and let X_D denote the Shimura curve attached to it. For any integer $N \geq 1$, let $X_0(N)$ be the modular curve of level N and $J_0(N) = \operatorname{Jac}(X_0(N))$. By $J_0(N)^{new}$, we shall denote the new part of $J_0(N)$ viewed as an optimal quotient of it. Ribet's isogeny theorem establishes the existence of a Hecke invariant isogeny

$$J_0(D)^{new} \to \operatorname{Jac}(X_D)$$

over $\mathbb{Q}$, though its proof relies on the fact that both abelian varieties have the same L-series and therefore is not explicit (cf. [18], see also [1]).

The problem of determining the possible kernels of the isogeny has been studied by Ogg in [17], the underlying idea being that the knowledge of the group of connected components of the Néron models of $J_0(D)^{new}$ and $\operatorname{Jac}(X_D)$ at a prime $p \mid D$ yields necessary conditions to be satisfied by the isogenies between them. As in [17], the component groups of $\operatorname{Jac}(X_D)$ can be handled by Raynaud's method and the theory of Čerednik-Drinfeld. However, the component groups of the optimal quotients $J_0(D)^{new}$ were only recently determined by Conrad and Stein in [4].

The aim of this section is to provide equations for the three Shimura genus two curves and to make Ribet's isogeny explicit for these examples.

Theorem 3.1. *The curves X_D with $D = 26, 38, 58$ are the unique Shimura curves of genus two. Moreover,*

(i) *Equations for the curves X_D are given in the following table:*

D	X_D
26	$y^2 = -2x^6 + 19x^4 - 24x^2 - 169$
38	$y^2 = -19x^6 - 82x^4 - 59x^2 - 16$
58	$2y^2 = -x^6 - 39x^4 - 431x^2 - 841$

(ii) *In all of three cases $J_0(D)^{new}$ is the Jacobian of a genus two curve C_D defined over $\mathbb{Q}$ and there is a cuspidal divisor $c(D)$ in $J_0(D)^{new}$ and an exact sequence*

$$0 \to \langle c(D) \rangle \to J_0(D)^{new} \to \mathrm{Jac}(X_D) \to 0.$$

Equations for the curves C_D, the cuspidal divisors $c(D)$ and their orders are given in the following table:

D	C_D	$c(D)$	$\lvert\langle c(D)\rangle\rvert$
26	$y^2 = 13x^6 + 10x^4 - 3x^2 - 4$	$(1/13) - (\infty)$	7
38	$y^2 = x^6 + 2x^4 + x^2 + 76$	$(1/19) - (\infty)$	5
58	$y^2 = x^6 + 6x^4 - 7x^2 + 16$	$(1/29) - (\infty)$	5

Proof. It follows from Ogg's list of hyperelliptic Shimura curves (cf. [16]) that $D = 26, 38$ and 58 are the only values of D for which $g(X_D) = 2$. These curves are bielliptic; more precisely, in Cremona's notation, by [19], it follows that for these values of D, $X_D/\langle w_2 \rangle$ is the elliptic curve $B2$ of conductor D while $X_{26}/\langle w_{13} \rangle$, $X_{38}/\langle w_{19} \rangle$, $X_{58}/\langle w_{58} \rangle$ are the elliptic curves $26A_1$, $38A_1$ and $58A_1$, respectively. It can be checked that for these values of D, the classes of isomorphism over $\bar{\mathbb{Q}}$ of both curves are different. Applying Proposition 2.1, we obtain that in all these cases the system (1) gives a unique genus two curve defined over $\mathbb{Q}$, which is given in the first table of the statement.

Let f_1 and f_2 be the two normalized newforms of $S_2(\Gamma_0(D))$ and let E_A and E_B be the elliptic curves over $\mathbb{Q}$ which are the strong Weil curve in the class of isogeny A and B respectively. We know that $J_0(D)^{new}$ and $E_A \times E_B$ are isogenous over $\mathbb{Q}$. We compute the following lattices of $\mathbb{C}$:

$$\Lambda_i = \{ \int_\gamma f_i(q) dq/q : \gamma \in H_1(X_0(D), \mathbb{Z}) \}, \quad 1 \leq i \leq 2,$$

and the lattice of $\mathbb{C}^2$:

$$\Lambda = \{ (\int_\gamma f_1(q) dq/q, \int_\gamma f_2(q) dq/q) : \gamma \in H_1(X_0(D), \mathbb{Z}) \}.$$

We obtain $(\Lambda_1 \times \Lambda_2)/\Lambda \simeq (\mathbb{Z}/2\mathbb{Z})^2$ with Λ being different from the lattices $(1/2 \cdot \Lambda_1) \times \Lambda_2$ and $\Lambda_1 \times (1/2 \cdot \Lambda_2)$. This result implies that there exists a nontrivial $G_{\mathbb{Q}}$-stable subgroup G of $E_A \times E_B$ isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$ such that $J_0(D)^{new} = (E_A \times E_B)/G$. In consequence, by [9], we know that $J_0(D)^{new}$ is the Jacobian of a genus two curve $C_D/\mathbb{Q}$ (of course, for $D = 26$, it was already known). Again, applying Proposition 2.1, we obtain a unique genus two curve defined over $\mathbb{Q}$, which is given in the table of the statement. Note that equations for $X_0(26)$ were already known (cf. [8]).

Now, we consider the morphism ϕ obtained as the composition of the following morphisms defined over $\mathbb{Q}$

$$J_0(D)^{new} \xrightarrow{\mu} E_A \times E_B \xrightarrow{\mathrm{id}_A \times \phi_B} E_A \times E_{B_2} \xrightarrow{\nu} \mathrm{Jac}(X_D),$$

where $\ker \mu, \ker \nu \simeq (\mathbb{Z}/2\mathbb{Z})^2$, id_A is the identity on E_A and ϕ_B is the cyclic isogeny from E_B to E_{B_2}. One can check (see [5]) that in all these cases the group $\ker(\mathrm{id}_A \times \phi_B)$ is a subgroup of $E_A(\mathbb{Q}) \times E_B(\mathbb{Q})$ of cardinality 7, 5, 5 depending on whether D is 26, 38 or 58 and, moreover, this group is the unique subgroup of rational points of $E_A(\mathbb{Q}) \times E_B(\mathbb{Q})$ with such a cardinality. Since $\mathrm{id}_A \times \phi_B$ has odd degree, this morphism maps the kernel of $\hat{\mu}$ to the kernel of ν because both

kernels are the unique nontrivial $G_{\mathbb{Q}}$-stable subgroups isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$ in their abelian varieties. Then, there is a morphism $\phi' : J_0(D)^{new} \to \mathrm{Jac}(X_D)$ such that $\phi = [2]\phi'$ and, thus, $|\ker \phi'| = |\ker(\mathrm{id}_A \times \phi_B)| = |\ker(\phi_B)|$.

Since D is square-free, we recall that cuspidal divisors are rational points in $J_0(D)$ and in particular in $J_0(D)^{new}$. The cuspidal divisors $c(D)$ given in the table have order 7, 15 and 35 in $J_0(D)$ for $D = 26, 38$ and 58 respectively. For the cases $D = 38$ and 58, we compute $(\int_{c(D)} f_1(q)dq/q, \int_{c(D)} f_2(q)dq/q) \in \mathbb{Q} \otimes \Lambda$ and check that its order in $(\mathbb{Q} \otimes \Lambda)/\Lambda$ is 5. This concludes the proof. □

Remark 3.1. *The three equations agree with the equations suggested in* [14]*. Moreover, Ogg suggested in* [17, p. 213]*, that the minimal degree of Ribet's isogeny should be the numerator of* $\frac{p+1}{12}$ *whenever* $D = 2p$*. This agrees with the table above. More precisely, when* $D = 26$*,* $(0) - (1/2) + (1/13) - (\infty) = 2(1/13) - 2(\infty)$ *in* $J_0(26)$*, which proves that the prediction done by Ogg in* [17] *about the kernel of this isogeny is again right.*

It can also be checked that for $D = 26, 38$ *the group* $\langle c(D) \rangle$ *is generated by* $3(0) - 3(\infty)$ *while for* $D = 58$ *it is generated by* $(0) - (\infty)$*, and in all three cases the kernel of the isogeny is a subgroup of* $\langle (0) - (\infty) \rangle$*. It would be interesting to know whether the pattern suggested by the examples holds in greater generality.*

Remark 3.2. *Theorem 3.1 provides an explicit model* $y^2 = ax^6 + bx^4 + cx^2 + d$ *for* X_{26}*,* X_{38} *and* X_{58} *which is known to have a cusp singularity at the only point* $P_\infty = [0 : 1 : 0]$ *of infinity. A smooth model of the curve is obtained by blowing up the point; the preimage of* P_∞ *by the normalizing map are two points and the coordinates of everyone of them generates* $\mathbb{Q}(\sqrt{a})$*. In the three cases above* $\mathbb{Q}(\sqrt{a})$ *is quadratic imaginary, as it was expected since Shimura curves fail to have real points* [24].

4. Explicit models of Atkin-Lehner quotients of Shimura curves

Let $D = p_1 \cdot \ldots \cdot p_{2r}$, $r \geq 1$, and $m \mid D$. Let $X_D^{(m)} = X_D/\langle \omega_m \rangle$ be the quotient of the Shimura curve X_D by the Atkin-Lehner involution ω_m.

Let $\mathbb{T} = \langle T_\ell, \omega_p : \ell \nmid D, p \mid D \rangle_{\mathbb{Q}}$ and $\underline{\mathbb{T}} = \langle \underline{T}_\ell, \underline{\omega}_p : \ell \nmid D, p \mid D \rangle_{\mathbb{Q}}$ denote the Hecke algebra regarded as $\mathbb{T} = \mathrm{End}_{\mathbb{Q}}(\mathrm{Jac}(X_D)) \otimes \mathbb{Q}$ and $\underline{\mathbb{T}} = \mathrm{End}_{\mathbb{Q}}(J_0(D)^{new}) \otimes \mathbb{Q}$, respectively. Ribet's isogeny $\mathrm{Jac}(X_D) \to J_0(D)^{new}$ provides an isomorphism between the vector spaces of regular differentials and identifies T_ℓ with $\underline{T}_\ell$ and ω_m with $\mu(m)\underline{\omega}_m$ for any $m \mid D$, where $\mu(m) = (-1)^{\sharp\{\text{primes } p \mid m\}}$.

Lemma 4.1. *The genus of* $X_D^{(m)}$ *is* 2 *if and only if* $(D, m) \in \{(35, 5), (39, 3), (51, 17), (55, 11), (57, 3), (62, 31), (65, 5), (65, 13), (69, 23), (74, 2), (74, 37), (82, 2), (85, 5), (85, 85), (86, 2), (86, 43), (87, 3), (91, 91), (93, 93), (94, 47), (106, 2), (115, 115), (118, 2), (122, 61), (123, 123), (129, 43), (141, 141), (142, 2), (142, 142), (155, 155), (158, 158), (161, 161), (166, 83), (178, 178), (183, 183), (237, 79), (254, 254), (326, 326), (446, 446)\}$.

Proof. Assume that the pair (D, m) is such that $g(X_D^{(m)}) = 2$. Since $\mathrm{Aut}(X_D^m) \supseteq W/\langle \omega_m \rangle \simeq (\mathbb{Z}/2\mathbb{Z})^{2r-1}$ and curves of genus two contain at most two copies of the cyclic group of order 2, it follows that necessarily $r = 1$ and hence $D = p \cdot q$.

Let $\ell \nmid D$ be a prime of good reduction of the curve. Following [16, §5], we obtain $\varphi(D)(\ell - 1)/12 \leq |\widetilde{X}_D(\mathbb{F}_{\ell^2})| \leq 2|\widetilde{X}_D^{(m)}(\mathbb{F}_{\ell^2})|$, where $\widetilde{X}_D$ denotes the special fiber of Morita's integral model of X_D over $\mathbb{Z}_\ell$. Since $\widetilde{X}_D^{(m)}$ is hyperelliptic, it admits a

map of degree 2 onto the projective line and hence $|\widetilde{X}_D^{(m)}(\mathbb{F}_{\ell^2})| \leq 2(\ell^2+1)$. Thus, $\varphi(D) \leq 48(\ell^2+1)/(\ell-1)$. Since $g(X_6)=0$, we may choose either $\ell=2$ or $\ell=3$ and hence $\varphi(D)\leq 240$. A computation of genera now yields the lemma. □

Proposition 4.2. *A Shimura curve $X_D^{(m)}$ of genus two admits a bielliptic involution if and only if $(D,m) \in \{(91,91),(123,123),(141,141),(142,2),(142,142),(155,155),(158,158),(254,254),(326,326),(446,446)\}$.*

In all these 10 cases, the hyperelliptic involution w on $X_D^{(m)}$ is not an Atkin-Lehner involution and $\mathrm{Aut}(X_D^{(m)}) = \langle w\rangle \times W/\langle\omega_m\rangle \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

Proof. By the same arguments as in [20], Proposition 1, since $\mathrm{Jac}(X_D^{(m)})$ is isogenous to a product of simple abelian varieties of real GL_2-type, it follows that the group of automorphisms of $X_D^{(m)}$ is abelian and only contains involutions defined over $\mathbb{Q}$.

As it is checked from the genus formulas in [16], the 10 cases in the above table are exactly those of Lemma 4.1 for which the single Atkin-Lehner involution u in $W/\langle\omega_m\rangle \subseteq \mathrm{Aut}(X_D^{(m)})$ is not the hyperelliptic involution w, and hence is bielliptic. Since $\langle w,u\rangle \subseteq \mathrm{Aut}(X_D^{(m)}) \simeq (\mathbb{Z}/2\mathbb{Z})^s$ for some $s\geq 1$ and $g(X_D^{(m)})=2$, it follows that $s\leq 2$ and hence $s=2$.

For the 29 remaining cases not quoted in Proposition 4.2, the single Atkin-Lehner involution in $W/\langle\omega_m\rangle \subseteq \mathrm{Aut}(X_D^{(m)})$ is the hyperelliptic involution of the genus two curve $X_D^{(m)}$. We know from Kuhn [12] that every quotient of a genus two curve $C/\mathbb{Q}$ by a nonhyperelliptic involution defined over $\mathbb{Q}$ has a rational point and thus is an elliptic curve over $\mathbb{Q}$.

Among these 29 curves, it turns out by checking Cremona tables, that their Jacobians are all simple over $\mathbb{Q}$ except for $(D,m)=(57,3),(106,2)$ and $(118,2)$. Indeed, this follows from the fact that these are the unique three cases such that there exist two different isogeny classes of elliptic curves of conductor D and invariant by $\mu(m)\underline{\omega}_m$. It is then clear that these 26 curves $X_D^{(m)}$ whose Jacobian is simple over $\mathbb{Q}$ can not be bielliptic. As for the values $(D,m)=(57,3),(106,2)$ and $(118,2)$ is concerned, there exactly two isogeny classes of elliptic curves of level D and invariant by $\mu(m)\underline{\omega}_m$. Namely, $57B, 57C$; $106A, 106C$; $118B, 118C$, respectively. For each possible choice of elliptic curves E and E' in these two isogeny classes, the abelian surface $E\times E'$ contains no nontrivial $G_{\mathbb{Q}}$-stable subgroups isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. In other words, the system (1) admits no rational solution and therefore, $X_D^{(m)}$ can not be a bielliptic curve. □

Theorem 4.3. *Equations for the curves in Proposition 4.2 and their elliptic quotients are given in the following table:*

$D = p \cdot q$	m	$X_D^{(m)}$	$X_D^{(m)}/\langle\omega_q\rangle$	$X_D^{(m)}/\langle w \cdot \omega_q\rangle$
$91 = 7 \cdot 13$	91	$y^2 = -x^6 + 19x^4 - 3x^2 + 1$	$91B1$	$91A1$
$123 = 3 \cdot 41$	123	$y^2 = -9x^6 + 19x^4 + 5x^2 + 1$	$123A1$	$123B1$
$141 = 3 \cdot 47$	141	$y^2 = 27x^6 - 5x^4 - 7x^2 + 1$	$141A1$	$141D1$
$142 = 2 \cdot 71$	2	$y^2 = -16x^6 - 87x^4 - 146x^2 - 71$	$142A1$	$142D2$
$142 = 2 \cdot 71$	142	$y^2 = 16x^6 + 9x^4 - 10x^2 + 1$	$142A1$	$142B1$
$155 = 5 \cdot 31$	155	$y^2 = 25x^6 - 19x^4 + 11x^2 - 1$	$155A1$	$155C1$
$158 = 2 \cdot 79$	158	$y^2 = -8x^6 + 9x^4 + 14x^2 + 1$	$158A1$	$158B1$
$254 = 2 \cdot 127$	254	$y^2 = 8x^6 + 25x^4 - 18x^2 + 1$	$254A1$	$254C1$
$326 = 2 \cdot 163$	326	$y^2 = x^6 + 10x^4 - 63x^2 + 4$	$326B1$	$326A1$
$446 = 2 \cdot 223$	446	$y^2 = -16x^6 - 7x^4 + 38x^2 + 1$	$446B1$	$446A1$

Moreover, for all these equations the action of w_q on them is $(x, y) \mapsto (-x, y)$.

Proof. We note that, in all 10 cases, it follows from Proposition 4.2 that $m = D$ except for the single case $(D, m) = (142, 2)$. Hence, the class of ω_q in $\mathrm{Aut}(X_D^{(m)})$ is the unique bielliptic involution of the curve that is of Atkin-Lehner type. We have split the proof in five parts in order to ease its reading.

Step 1: Isogeny and isomorphism classes of the elliptic quotients.

We firstly determine the isogeny classes of the elliptic curves $E = X_D^{(m)}/\langle\omega_q\rangle$ and $E' = X_D^{(m)}/\langle w \cdot \omega_q\rangle$ of conductor D. There are exactly two normalized newforms f, f' for $\Gamma_0(D)$ with rational Fourier coefficients whose signs of the eigenvalues for the action of the Atkin-Lehner involutions are the following, depending on whether $m = D$ or $m = p$:

$m = D$	$\underline{\omega_p}$	$\underline{\omega_q}$
f	$-$	$-$
f'	$+$	$+$

$m = p$	$\underline{\omega_p}$	$\underline{\omega_q}$
f	$-$	$-$
f'	$-$	$+$

Then, the elliptic curves E and E' are isogenous to A_f and A'_f over $\mathbb{Q}$, respectively. An examination of the 10 cases shows that, for $(D, m) \in \{(141, 141), (142, 142), (158, 158), (326, 326), (446, 446)\}$, the isomorphism classes of E and E' over $\mathbb{Q}$ are determined, because every isogeny class contains a single isomorphism class. These are quoted in the table of the statement. For the remaining cases, we have the following possibilities:

(D, m)	E	E'
$(91, 91)$	B_1, B_2, B_3	A_1
$(123, 123)$	A_1, A_2	B_1
$(142, 2)$	A_1	D_1, D_2
$(155, 155)$	A_1, A_2	C_1
$(254, 254)$	A_1, A_2, A_3	C_1

Step 2: Candidate equations.

We now proceed to determine a finite set of candidate equations for the 10 curves $X_D^{(m)}$. We do so by applying Proposition 2.1 to every possible pair (E, E') obtained in Step 1. For every pair, it turns out that system (1) yields one rational solution. This means that, in the five cases (D, m) where there is a single possibility for

(E, E'), we have already determined an equation for the curve $X_D^{(m)}$, as quoted in Theorem 4.3. In the five remaining cases, we obtain the following candidates:

(D,m)	(E,E')	$C:$	ay^2	$=$	$f(x)$
$(91,91)$	(B_1,A_1)	$C_{91,1}:$	y^2	$=$	$-x^6+19x^4-3x^2+1$
	(B_2,A_1)	$C_{91,2}:$	y^2	$=$	$91x^6+43x^4+9x^2+1$
	(B_3,A_1)	$C_{91,3}:$	$5y^2$	$=$	$2401x^6-403x^4+3x^4-1$
$(123,123)$	(A_1,B_1)	$C_{123,1}:$	y^2	$=$	$-9x^6+19x^4+5x^2+1$
	(A_2,B_1)	$C_{123,2}:$	y^2	$=$	$1681x^6-419x^4+35x^2-1$
$(142,2)$	(A_1,D_1)	$C_{142,1}:$	y^2	$=$	$8x^6+33x^4+22x^2+1$
	(A_1,D_2)	$C_{142,2}:$	y^2	$=$	$-16x^6-87x^4-146x^2-71$
$(155,155)$	(A_1,C_1)	$C_{155,1}:$	y^2	$=$	$25x^6-19x^4+11x^2-1$
	(A_2,C_1)	$C_{155,2}:$	$3y^2$	$=$	$961x^6-483x^4-45x^2-1$
$(254,254)$	(A_1,C_1)	$C_{254,1}:$	y^2	$=$	$8x^6+25x^4-18x^2+1$
	(A_2,C_1)	$C_{254,2}:$	y^2	$=$	$127x^6-461x^4-51x^2+1$
	(A_3,C_1)	$C_{254,3}:$	$71y^2$	$=$	$x^6-76888x^4-891x^2+2$

These equations have been computed such that the bielliptic involution ω_q acts as $(x,y)\mapsto(-x,y)$ and hence its two fixed points are those whose x-coordinates are 0. We devote the rest of the proof to discard the wrong equations for $X_D^{(m)}$ from the above in the table, by using suitable sieves.

Step 3: The sieve of Heegner points fixed by the involutions.

Let us only consider in this part the four cases when $m=D$. From Proposition 4.2, $\mathrm{Aut}(X_D^{(D)})=\langle\omega_q,w\rangle$. The two fixed points P, Q of ω_q acting on $X_D^{(D)}$ are the projection from X_D onto $X_D^{(D)}$ of the four points fixed by ω_p, when we regard it as an automorphism of X_D. When $h(-4p)=1$, it follows from the class field theory on Heegner points (cf. [10]) that P, $Q\in X_D^{(D)}(\mathbb{Q})$. When $h(-4p)=2$, it follows that P, $Q\in X_D^{(D)}(K)$, where K is a quadratic field such that $K(\sqrt{-p})$ is the Hilbert class field of $\mathbb{Q}(\sqrt{-p})$. We thus obtain that, when $(D,m)=(91,91)$, $(123,123)$ or $(254,254)$ the fixed points P, Q lie on $X_D^{(D)}(\mathbb{Q})$, whereas when $(D,m)=(155,155)$, P, $Q\in X_{155}^{(155)}(K)$ for either $K=\mathbb{Q}(\sqrt{5})$ or $\mathbb{Q}(\sqrt{-1})$.

On the other hand, on the bielliptic model $ay^2=bx^6+cx^4+dx^2+e$, the coordinates of the two points fixed by ω_q generate $\mathbb{Q}(\sqrt{e/a})$. This allows us to discard the equations $C_{91,3}$, $C_{123,2}$, $C_{155,2}$ and $C_{254,3}$. We have thus already determined an equation for $X_{123}^{(123)}$ and $X_{155}^{(155)}$.

Step 4: The real points sieve.

Shimura proved in [24] that $X_D(\mathbb{R})=\emptyset$. Later, Ogg [16] studied the question whether the Atkin-Lehner quotients of Shimura curves admit real points. Namely, he proved that $X_D^{(m)}(\mathbb{R})\neq\emptyset$ if and only if $(\frac{m}{p})\neq 1$ for all $p\mid D$, $p\nmid m$.

Since $(\frac{2}{71})=1$, we deduce that $X_{142}^{(2)}(\mathbb{R})=\emptyset$ and hence $X_{142}^{(2)}\simeq C_{142,2}$ over $\mathbb{Q}$.

Step 5: The Čerednik-Drinfeld sieve.

Let us recall the theory of Čerednik-Drinfeld on the bad reduction of the Atkin-Lehner quotients $X_D^{(m)}$ at a fixed prime $p\mid D$ (cf. [2], [11], [13], [17]).

Let K_p denote the quadratic unramified extension of $\mathbb{Q}_p$ and let R_p be its ring of integers. Over K_p, the curves X_D are generalized Mumford curves that admit a

p-adic uniformization by a Schottky group which is often non-torsion-free. In the terminology of [11], these are called admissible curves.

Let $h(\delta,\nu)$ denote the class number of a quaternion Eichler order of level ν in a quaternion algebra of discriminant δ over $\mathbb{Q}$. As shown in [13], X_D admits a proper but often non regular integral model $\mathcal{X}_D$ over R_p whose special fibre $\widetilde{X}_D/\mathbb{F}_{p^2}$ is the union of $2h(\frac{D}{p},1)$ irreducible rational components meeting transversally at a total number of $h(\frac{D}{p},p)$ points. The intersection points of the special fibre are the only possible non regular points of $\mathcal{X}_D$ and the only allowed multiplicities are $m=1,2$ and 3. The reduction type of $\mathcal{X}_D$ at p is described by a weighted graph by interpreting each component as a vertex, an intersection point P between two components as an edge joining the two vertices and the multiplicity m of P as the weight of the edge.

For every prime $q\leq 13$, it turns out that the dual graph of X_{pq} at p consists of exactly two vertices joined by $g(X_{pq})+1$ edges.

Moreover, the Atkin-Lehner involution ω_{pq} lifts to $\mathcal{X}_D$ and switches the two vertices and the quotient graph consists of a single vertex with several loops of multiplicity $1,2$ or 3 around it. In consequence, the special fibre of $\mathcal{X}_D/\langle\omega_{pq}\rangle$ has a single and possibly singular irreducible component. After blowing up the non regular closed points of $\mathcal{X}_D/\langle\omega_{pq}\rangle$ as in [13, p. 288], we deduce that any two irreducible components of the special fibre of the minimal regular model of $X_D^{(m)}$ meet at most at two different intersection points.

We can contrast this information with the explicit computation of the reduction type of the equations in the above tables at the primes $p\mid D$. This can be accomplished by means of Liu's package *genus2reduction*, that computes the minimal regular model of any curve of genus 2 over $\mathbb{Q}$ over $\mathbb{Z}[\frac{1}{2}]$.

The reduction type of $C_{91,1}$ and $C_{91,2}$ at $p=7$ are $I_{\{1-1-0\}}$ and $I_{\{1-1-1\}}$, respectively. It follows from [15], the former is the symbol for a single irreducible rational component with two nodes while the latter corresponds to two rational components meeting at three points. Hence, we discard $C_{91,2}$ and conclude that $X_{91}^{(91)}\simeq C_{91,1}$. Similarly, the reduction type of $C_{254,1}$ and $C_{254,2}$ at $p=127$ are $I_{\{1-1-0\}}$ and $I_{\{1-1-1\}}$, respectively. This allows us to show that $X_{254}^{(254)}\simeq C_{254,1}$. □

Acknowledgements. The first author thanks the Number Theory Group of the University of Nottingham for the warm hospitality during the spring semester of 2003.

References

[1] A. Arenas, On the traces of Hecke operators, *J. Number Theory* **100** (2003), 307-312.
[2] S. Baba, Shimura curve quotients with odd Jacobian, J. Number Theory **87** (2001), 96-108.
[3] P. Bayer, Uniformization of certain Shimura curves, in *Differential Galois Theory*, Banach Center Publications, **58**, Polish Academy of Sciences, 2002.
[4] B. Conrad, W. Stein, Component groups of purely toric quotients, Math. Research Letters **8** (2001), 745-766.
[5] J. E. Cremona, *Algorithms for modular elliptic curves*, Cambridge Univ. Press, Cambridge, UK,1992.
[6] N. Elkies, Shimura Curve Computations, *Lect. Notes Comp. Sc.* **1423**, Proceedings of ANTS-3, 1998; J.P.Buhler, ed. , 1-49.

[7] E. González-Jiménez, J. González, Modular curves of genus 2, *Math. Comp.* **72 (241)** (2003), 397-418.
[8] J. González Rovira, Equations of hyperelliptic modular curves, *Ann. Inst. Fourier (Grenoble)* **41 (4)** (1991), 779-795.
[9] E. W. Howe, F. Leprévost ans B. Poonen, Large torsion subgroups of split Jacobians of curves of genus two or three, *Forum Math.* **12** (2000), 315-364.
[10] B. W. Jordan, *On the Diophantine arithmetic of Shimura curves*, Harvard Ph. D. Thesis, 1981.
[11] B. W. Jordan, R. Livné, Local diophantine properties of Shimura curves, *Math. Ann.* **270** (1985), 235-248.
[12] R. M. Kuhn, Curves of genus 2 with split jacobian, *Trans. Amer. Math. Soc.* **307** (1988), 41-49.
[13] A. Kurihara, On some examples of equations defining Shimura curves and the Mumford uniformization, *J. Fac. Sci. Univ. Tokyo, Sec. IA* **25** (1979), 277-301.
[14] A. Kurihara, On p-adic Poincaré series and Shimura curves, *Intern. J. Math.* **5** (1994), 747-763.
[15] Y. Namikawa, K. Ueno, The complete classification of fibres in pencils of curves of genus two, *Manuscripta Math.* **9** (1973), 143-186.
[16] A. P. Ogg, Real points on Shimura curves, *Arithmetic and geometry*, Progr. Math. **35**, Birkhäuser Boston, Boston, MA, (1983), 277-307.
[17] A. P. Ogg, Mauvaise réduction des courbes de Shimura, *Séminaire de théorie des nombres*, Progr. Math. **59** Birkhäuser Boston, Boston, MA, (1983-84), 199-217.
[18] K. A. Ribet, Sur les varietés abéliennes à multiplications réelles, *C. R. Acad. Sc. Paris* **291** (1980), 121-123.
[19] D. P. Roberts, *Shimura curves analogous to* $X_0(N)$, Harvard Ph. D. Thesis, 1989.
[20] V. Rotger, On the group of automorphisms of Shimura curves and applications, *Compos. Math.* **132** (2002), 229-241.
[21] V. Rotger, Modular Shimura varieties and forgetful maps, to appear in *Trans. Amer. Math. Soc.*
[22] V. Rotger, Shimura curves embedded in Igusa's threefold, to appear in *Modular curves and abelian varieties*, Progress in Mathematics, Birkhõuser.
[23] G. Shimura, Construction of class fields and zeta functions of algebraic curves, *Ann. Math.* **85** (1967), 58-159.
[24] G. Shimura, On the real points of an arithmetic quotient of a bounded symmetric domain, *Math. Ann.* **215** (1975), 135-164.

Universitat Politècnica de Catalunya, Departament de Matemàtica Aplicada IV (EUPVG), Av. Victor Balaguer s/n, 08800 Vilanova i la Geltrú, Spain.
E-mail address: josepg@mat.upc.es,vrotger@mat.upc.es